

**In the Claims:**

1. (Previously Presented) A method for secure communication comprising:  
generating a plurality of virtual private proxies based on an agreement between a first entity and a second entity;

associating a first virtual private proxy of the plurality of virtual private proxies with the first entity and a second virtual private proxy of the plurality of virtual private proxies with the second entity;

monitoring data at the first virtual private proxy associated with the first entity;

determining whether the data violates the agreement; and

disallowing communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

2. (Currently Amended) The method for secure communication according to Claim 1, wherein determining whether the data violates the agreement comprises:

determining whether the data includes a security violation.

~~examining the data with respect to the agreement at the first virtual private proxy;~~

~~determining whether the data is allowed by the agreement; and~~

~~indicating a violation when the data does not conform to the agreement.~~

3. (Currently Amended) The method for secure communication according to Claim 2, wherein the security violation is a virus or malicious program. ~~generating the violation comprises:~~

~~generating an alarm based on the violation;~~

~~communicating the alarm to an appropriate entity; and~~

~~logging the violation.~~

4. (Currently Amended) The method for secure communication according to ~~Claim 2~~ Claim 3, wherein the security violation is an intrusion attempt. ~~the appropriate entity is a systems administrator and wherein disallowing the data comprises discarding the data when the data violates the agreement.~~

5. (Currently Amended) The method for secure communication according to Claim 1, Claim 3, wherein the alarm comprises information associated with the violation, further comprising:

hiding the existence of at least one of the first virtual private proxy or the second virtual private proxy to entities other than the first entity and the second entity of the agreement.

6. (Cancelled)

7. (Cancelled)

8. (Original) The method for secure communication according to Claim 1, wherein the agreement comprises types of data allowed.

9. (Original) The method for secure communication according to Claim 8, wherein the agreement further comprises a transport protocol indication and a transport security protocol indication and wherein the type of data allowed comprises XML data.

10. (Original) The method for secure communication according to Claim 9, wherein the agreement further comprises a document exchange protocol indication and a process specification document indication.

11. (Cancelled)

12. (Cancelled)

13. (Cancelled)

14. (Previously Presented A system for secure communication comprising:

logic stored on a medium and configured to:

generate a plurality of virtual private proxies based on an agreement between a first entity and a second entity;

associate a first virtual private proxy of the plurality of virtual private proxies with the first entity and a second virtual private proxy of the plurality of virtual private proxies with the second entity;

monitor data at the first virtual private proxy associated with the first entity;

determine whether the data violates the agreement; and

disallow communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Currently Amended) The system for secure communication according to Claim 14, ~~wherein the agreement comprises types of data allowed.~~ wherein the logic is further configured to:

receive a first profile from the first entity,

receive a second profile from the second entity, and

automatically generate the agreement based on the first profile and the second profile.

22. (Original) The system for secure communication according to Claim 21, wherein the agreement further comprises a transport protocol indication and a transport security protocol indication and wherein the type of data allowed comprises XML data.

23. (Original) The system for secure communication according to Claim 22, wherein the agreement further comprises a document exchange protocol indication and a process specification document indication.

24. (Currently Amended) The system method for secure communication according to Claim 14, wherein the logic is ~~further configured to monitor data received at the first virtual private proxy from the first entity.~~ in determining whether the data violates the agreement determines whether the data includes an intrusion attempt.

25. (Currently Amended) The system method for secure communication according to Claim 14, wherein the logic is ~~further configured to monitor data received at the first virtual private proxy to be communicated to the first entity.~~ in determining whether the data violates the agreement determines whether the data includes a virus or malicious program.

26. (Original) A method for secure communication comprising:  
generating a first virtual private proxy associated with a first entity;  
generating a second virtual private proxy associated with a second entity;  
monitoring communications between the first virtual private proxy and the second  
virtual private proxy based on an agreement for electronic data exchange between the first  
and second entities; and  
responding to violations of the agreement based on the agreement.

27. (Original) The method according to Claim 26 and further comprising:  
determining a first profile associated with the first entity;  
determining a second profile associated with the second entity; and  
automatically generating the agreement based on the first and second profiles.

28. (Original) The method according to Claim 26 and further comprising:  
linking the first virtual private proxy to the second virtual private proxy over a link;  
and  
communicating data between the first virtual private proxy and the second virtual  
private proxy over the link.

29. (Original) The method according to Claim 28, wherein the link comprises  
a logical data link at a secure switch.

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Previously Presented) The method according to Claim 27, wherein the first  
profile comprises at least one indication of business information associated with the first  
entity.

34. (Previously Presented) The method according to Claim 27, wherein the first profile comprises a transport protocol and a messaging protocol.

35. (Original) The method according to Claim 34, wherein the first profile further comprises a transport security protocol and a specification document.

36. (Original) The method according to Claim 35, wherein the first profile further comprises a name and contact information associated with the first entity.

37. (Original) The method according to Claim 26, wherein determining the violation comprises:

- examining the data with respect to the agreement at the first virtual private proxy;
- determining whether the data is allowed by the agreement;
- determining the violation when the data is not allowed by the agreement; and
- communicating the data to the second virtual private proxy when the data is allowed by the agreement.

38. (Original) The method according to Claim 26, wherein responding to the violation comprises:

- generating an alarm based on the violation;
- logging the violation; and
- discarding the data associated with the violation.

39. (Original) The method according to Claim 38, wherein responding to the violation further comprises forbidding communication between the first virtual private proxy and the second virtual private proxy.

ATTORNEY DOCKET NO  
021768.1152

PATENT APPLICATION  
10/040,573

8

40. (Cancelled)

41. (Previously Presented) A system for secure communication comprising:  
logic stored on storage and configured to:  
generate a first virtual private proxy associated with a first entity;  
generate a second virtual private proxy associated with a second entity;  
monitor communications between the first virtual private proxy and the second  
virtual private proxy based on an agreement for electronic data exchange between the first  
and second entities; and  
respond to violations of the agreement based on the agreement.

42. (Previously Presented) The system according to Claim 41, wherein the logic is  
further configured to:  
determine a first profile associated with the first entity;  
determine a second profile associated with the second entity; and  
automatically generate the agreement based on the first and second profiles.

43. (Previously Presented) The system according to Claim 41, wherein the logic is  
further configured to:  
link the first virtual private proxy to the second virtual private proxy over a link; and  
communicate data between the first virtual private proxy and the second virtual  
private proxy over the link.

44. (Cancelled)

45. (Cancelled)

46. (Cancelled)

47. (Currently Amended) The system according to Claim 41, wherein the ~~first and  
second entities respectively comprise a business.~~ logic is further configured to:  
hide the existence of at least one of the first virtual private proxy or the second virtual  
private proxy to entities other than the first entity and the second entity of the agreement.



48. (Previously Presented) The system according to Claim 42, wherein the first profile comprises at least one indication of business information associated with the first entity.

49. (Previously Presented) The system according to Claim 42, wherein the first profile comprises a transport protocol and a messaging protocol.

50. (Original) The system according to Claim 49, wherein the first profile further comprises a transport security protocol and a specification document.

51. (Original) The system according to Claim 50, wherein the first profile further comprises a name and contact information associated with the first entity.

52. (Currently Amended) The system according to Claim 41, wherein the agreement prohibits viruses or malicious programs. ~~logic is further configured to:~~  
~~examine the data with respect to the agreement at the first virtual private proxy;~~  
~~determine whether the data is allowed by the agreement;~~  
~~determine the violation when the data is not allowed by the agreement; and~~  
~~communicate the data to the second virtual private proxy when the data is allowed by the agreement.~~

53. (Currently Amended) The system according to Claim 41, wherein the agreement prohibits intrusion attempts. ~~the logic is further configured to:~~  
~~generate an alarm based on the violation;~~  
~~log the violation; and~~  
~~discard the data associated with the violation.~~

54. (Previously Presented) The system according to Claim 53, wherein the logic is further configured to forbid communication between the first virtual private proxy and the second virtual private proxy.

55. (Previously Presented) A method for secure communication comprising:

- generating a plurality of virtual private proxies based on an agreement between a first entity and a second entity;
- wherein the agreement further comprises a document exchange protocol indication and a process specification document indication;
- associating a first virtual private proxy of the plurality of virtual private proxies with the first entity and a second virtual private proxy of the plurality of virtual private proxies with the second entity;
- wherein the first virtual private proxy comprises a logical representation of a logical access point between the first entity and a secure switch;
- monitoring data at the first virtual private proxy associated with the first entity;
- examining the data with respect to the agreement at the first virtual private proxy;
- determining whether the data is allowed by the agreement;
- indicating a violation when the data does not conform to the agreement; and
- disallowing communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

56. (New ) A method for secure communication, the method comprising:  
communicating a profile to a secure switch, the profile specifying parameters of communication;  
initiating a connection with a secure switch; and  
receiving data through a first virtual private proxy of the secure switch that complies with the parameters specified by the profile.

57. (New ) The method of Claim 56, wherein the communicating, initiating, and receiving are carried out on a first entity and the profile is associated with the first entity.

58. (New ) The method of Claim 57, further comprising:  
receiving, at the first entity, a communication initiation request from a remote computer; and  
facilitating communication between the remote computer and a second entity.

59. (New ) The method of Claim 57, further comprising:  
communicating data, from the first entity, to a second entity through the secure switch.

60. (New ) The method of Claim 59, further comprising:  
receiving an indication from the secure switch that the communicated data does not comply with parameters specified by a profile of the second entity.

61. (New ) The method of Claim 57, wherein the received data is communicated from a second entity through the secure switch.

62. (New ) The method of Claim 56, wherein the profile is used in a Collaboration Profile Agreement.

63. (New ) The method of Claim 56, wherein the profiles specifies a type of data.

64. (New ) The method of Claim 56, wherein the profiles prohibits viruses or malicious programs.

65. (New ) The method of Claim 56, wherein the profiles prohibits intrusion attempts.

66. (New ) The method of Claim 56, wherein the connection is a secure connection.

67. (New ) A system for secure communication comprising:  
logic stored on computer readable media and configured to:  
communicate a profile to a secure switch, the profile specifying parameters of  
communication;  
initiate a connection with a secure switch; and  
receive data through a first virtual private proxy of the secure switch that complies  
with the parameters specified by the profile.
68. (New ) The system of Claim 67, wherein the logic is associated with a first  
entity.
69. (New ) The system of Claim 68, wherein the logic is further configured to:  
receive a communication initiation request from a remote computer; and  
facilitate communication between the remote computer and a second entity.
70. (New ) The system of Claim 68, wherein the logic is further configured to:  
receive an indication from the secure switch that the communicated data does not  
comply with parameters specified by a profile of the second entity.
71. (New ) The system of Claim 67, wherein the profiles specifies a type of data.
72. (New ) The system of Claim 67, wherein the profiles prohibits viruses or  
malicious programs.
73. (New ) The system of Claim 67, wherein the profiles prohibits intrusion  
attempts.